RECIPES FOR TERNARY DIOPHANTINE EQUATIONS OF SIGNATURE (p, p, k) (Diophantine Problems and Analytic Number Theory)

AUTHOR(S):

Bennett, Michael A.

数理解析研究所講究録 1319 巻 2003 年 51-55

RECIPES FOR TERNARY DIOPHANTINE EQUATIONS OF SIGNATURE (p, p, k)

MICHAEL A. BENNETT

ABSTRACT. In this paper, we survey recent work on ternary Diophantine equations of the shape $Ax^n + By^n = Cz^m$ for $m \in \{2, 3, n\}$ where $n \geq 5$ is prime. Our goal is to provide a simple procedure which, given A, B, C and m, enables us to decide whether techniques based on the theory of Galois representations and modular forms suffice to ensure that corresponding ternary equations lack nontrivial solutions in integers x, y, z and prime $n \geq 5$.

1. INTRODUCTION

Inspired by the work of Wiles [19] and, subsequently, Breuil, Conrad, Diamond and Taylor [3], there has been a great deal of research focussing on ternary Diophantine equations from the perspective of (modular) elliptic curves and related Galois representations and modular forms (see e.g. [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [17]). These have, for the most part been concerned with equations of the shape

$$Ax^p + By^q = Cz^r$$

for p, q and r positive integers with $1/p + 1/q + 1/r < 1$. We refer to the triple (p, q, r) as the *signature* of the corresponding equation. In this paper, we will provide "recipes" for solving such equations under very special conditions, in case

$$(p, q, r) = (n, n, 2), (n, n, 3), (n, n, n).$$

where $n \geq 5$ is prime. This, primarily, catalogues prior work of Darmon [5], Darmon and Merel [8], the author and Skinner [1], the author, Vatsal and Yazdani [2], and of Kraus [13].

2. ASSUMPTIONS

In the sequel, we will always assume that $n \geq 5$ is prime and that a, b, c, A, B and C are nonzero integers with aA, bB and cC pairwise coprime, $ab \neq \pm 1$, satisfying

$$Aa^n + Bb^n = Cc^m \text{ with } m \in \{2, 3, n\}. \tag{1}$$

For future use, we will define, for a given prime q and nonzero integer x,

$$\mathrm{Rad}_q(x) = \prod_{p \mid x, p \neq q} p$$

where the product is over p prime, and write $\mathrm{ord}_q(x)$ for the largest nonegative integer k such that q^k divides x.

Supported in part by a grant from NSERC.

2.1. **Signature** $(n, n, 2)$. In case $m = 2$, we will assume further that $n \geq 7$ and, without loss of generality, that aA is odd and that C is squarefree. Further, if $ab \equiv 1 \pmod 2$ and $\mathrm{ord}_2(B) = 2$, we suppose, again without loss of generality, that $c \equiv -bB/4 \pmod 4$.

Then, to a solution to (1), we associate a positive integer N, by

$$N = \mathrm{Rad}_2(AB)\,\mathrm{Rad}_2(C)^2\,\epsilon_2, \tag{2}$$

where

$$\epsilon_2 = \begin{cases} 1 & \text{if } \mathrm{ord}_2(Bb^n) = 6 \\ 2 & \text{if } \mathrm{ord}_2(Bb^n) \geq 7 \\ 4 & \text{if } \mathrm{ord}_2(B) = 2 \text{ and } b \equiv -BC/4 \pmod 4 \\ 8 & \text{if } \mathrm{ord}_2(B) = 2 \text{ and } b \equiv BC/4 \pmod 4, \text{ or if } \mathrm{ord}_2(B) \in \{4, 5\} \\ 32 & \text{if } \mathrm{ord}_2(B) = 3 \text{ or if } bBC \text{ is odd} \\ 128 & \text{if } \mathrm{ord}_2(B) = 1 \\ 256 & \text{if } C \text{ is even.} \end{cases}$$

2.2. **Signature** $(n, n, 3)$. If $m = 3$, we assume, without loss of generality, that $Aa \not\equiv 0 \pmod 3$ and $Bb^n \not\equiv 2 \pmod 3$. Further, suppose that C is cube free, without loss of generality, that A and B are nth-power free and that equation (1) does not correspond to the identity

$$1 \cdot 2^5 + 27 \cdot (-1)^5 = 5 \cdot 1^3. \tag{3}$$

In this situation, we define N by

$$N = \mathrm{Rad}_3(AB)\,\mathrm{Rad}_3(C)^2\,\epsilon_3, \tag{4}$$

where

$$\epsilon_3 = \begin{cases} 1 & \text{if } \mathrm{ord}_3(Bb^n) = 3, \\ 3 & \text{if } \mathrm{ord}_3(Bb^n) > 3, \\ 9 & \text{if } \mathrm{ord}_3(Bb^n) = 2 \text{ or if } 9 \mid (2 + C^2Bb^n - 3Cc), \\ 27 & \text{if } 3 \| (2 + C^2Bb^n - 3Cc) \text{ or if } \mathrm{ord}_3(Bb^n) = 1, \\ 81 & \text{if } 3 \mid C. \end{cases}$$

2.3. **Signature** (n, n, n). Finally, if $m = n$, we define N by

$$N = \mathrm{Rad}_2(ABC)\,\epsilon_n, \tag{5}$$

where

$$\epsilon_n = \begin{cases} 1 & \text{if } \mathrm{ord}_2(ABC) = 4, \\ 2 & \text{if } \mathrm{ord}_2(ABC) = 0 \text{ or if } \mathrm{ord}_2(ABC) \geq 5, \\ 8 & \text{if } \mathrm{ord}_2(ABC) = 2 \text{ or } 3, \\ 32 & \text{if } \mathrm{ord}_2(ABC) = 1. \end{cases}$$

3. The main result

Proposition 3.1. *Suppose that a, b, c, A, B and C are nonzero integers with aA, bB and cC pairwise coprime, $ab \neq \pm 1$, satisfying*

$$Aa^n + Bb^n = Cc^m$$

with $n \geq 5$ (for $m \in \{3, n\}$) or $n \geq 7$ (if $m = 2$) where, in each case, n is prime. Suppose further, that the equation does not correspond to (3). Then there exists a cuspidal newform $f = \sum_{r=1}^{\infty} c_r q^r$ of weight 2, trivial Nebentypus character and level N for N as given in (2) (if $m = 2$), (4) (if $m = 3$) or (5) (if $m = n$). Moreover, if we write K_f for the field of definition of the Fourier coefficients c_r of the form f and suppose that p is a prime, coprime to nN, then

$$Norm_{K_f/\mathbb{Q}}(c_p - a_p) \equiv 0 \pmod{n}, \tag{6}$$

where $a_p = \pm(p+1)$ or $a_p \in S_{p,m}$, with

$$S_{p,2} = \{x : |x| < 2\sqrt{p},\ x \equiv 0 \pmod 2\},$$

$$S_{p,3} = \{x : |x| < 2\sqrt{p},\ x \equiv p+1 \pmod 3\}$$

and

$$S_{p,n} = \{x : |x| < 2\sqrt{p},\ x \equiv p+1 \pmod 4\}.$$

This combines work from [1], [2] and [13]. In the case of signature $(n, n, 3)$, it is a slightly less precise version of the analogous statement in [2].

4. Some useful propositions

In this section, we will collect a variety of results that enable us, under certain assumptions, to deduce a contradiction from Proposition 3.1. They are as follows :

Proposition 4.1. *There are no weight 2, level N cuspidal newforms with trivial character for*

$$N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60\}.$$

Proposition 4.2. *Suppose that $m = 2$ or $m = 3$ and that $n \geq 5$ (if $m = 3$) or $n \geq 7$ (if $m = 2$) where, in each case, n is prime. Then the form f can have CM by an imaginary quadratic field K only if one of the following holds:*

(a) *$ab = \pm 2^r$, $r > 0$, 2 $\not|$ ABC, and 2 splits in K.*
(b) *$n = 5, 7$ or 13, n splits in K, and either the modular Jacobian $J_0(mn)$ has no quotient of rank 0 over K, or $ab = \pm 2^r 3^s$ with $s > 0$ and 3 ramifies in the field K.*

Proposition 4.3. *Suppose that $m = 2$ or $m = 3$ and that $n \geq 5$ (if $m = 3$) or $n \geq 7$ (if $m = 2$) where, in each case, n is prime. Then the form f cannot correspond to an elliptic curve E over $\mathbb{Q}$ for which the j-invariant $j(E)$ is divisible by any odd prime $p \neq n$ dividing C.*

These propositions are, essentially, available in [1], [2] and [13]. The reader is directed to these papers and to the surveys [14] and [15] for detailed explanations of the methods involved in their proofs.

5. An example or two

In this section, we will indicate how the preceding propositions may be employed to show that certain Diophantine equations lack "nontrivial" solutions. Let us begin by showing that the equation

$$x^n + y^n = 5z^2 \tag{7}$$

has no solutions in nonzero integers x, y, z, provided $n \geq 7$ is prime (the cases $n = 4, 5, 6, 9$ may be treated via different methods, such as those of Coleman-Chabauty; see e.g [16]). Suppose that (a, b, c) is a solution to (7) with $n \geq 7$ prime and $abc \neq 0$. We distinguish two cases, according to whether ab is even or odd. In the first instance, we have $N = 50$. There are just two newforms of this level, corresponding to elliptic curves over $\mathbb{Q}$. Each of these forms has $c_3 = \pm 1$, contradicting (6) (since $a_3 \in \{0, \pm 2, \pm 4\}$).

If ab is odd, then we have from (2) that $N = 800$. From Stein's tables [18], we find that there are 14 Galois conjugacy classes of forms at this level; we list some Hecke eigenvalues for a number of these :

newform	c_p
800, 2	$c_3 = 1$
800, 5	$c_3 = 1$
800, 6	$c_3 = -1$
800, 9	$c_3 = -1$
800, 10	$c_3 = \pm\sqrt{5}, c_{19} = \mp 3\sqrt{5}$
800, 11	$c_3 = 1 \pm \sqrt{5}$
800, 12	$c_3 = \pm 2\sqrt{2}$
800, 13	$c_3 = \pm\sqrt{5}, c_{19} = \pm 3\sqrt{5}$
800, 14	$c_3 = -1 \pm \sqrt{5}$

Here, we refer to forms via Stein's numbering system [18]. For the forms in the above table, considering c_3, congruence (6) contradicts $n \geq 7$ prime, except possibly for those forms in the classes 800,10 and 800,13. For such forms $c_3 = \pm\sqrt{5}$ and so, from (6), n must divide one of $-5, -1, 11$. Since $n \geq 7$ it must be that $n = 11$. For these forms we also have $c_{19} = \pm 3\sqrt{5}$, whence, again by (6), 11 must divide one of $-45, -41, -29, -9, 36, 355$. Since this fails to occur, none of the forms in the classes 800,10 and 800,13 can be the f whose existence is guaranteed by Proposition 3.1.

Next, we observe that the forms 800,3 and 800,7 correspond to isogeny classes of elliptic curves having j-invariants

$$j = 438976/5 \quad \text{or} \quad -64/25.$$

Proposition 4.3 implies that f is neither of these forms.

Finally, the forms 800,1, 800,4 and 800,8 each correspond to isogeny classes of elliptic curves having complex multiplication by $\mathbb{Q}(\sqrt{-1})$ (hence the corresponding newforms have CM by $\mathbb{Q}(\sqrt{-1})$). Invoking Proposition 4.2, it follows that $n = 7$ or 13 and that n splits in $\mathbb{Q}(\sqrt{-1})$. This implies that $n = 13$ and, since 3 does not ramify in $\mathbb{Q}(\sqrt{-1})$, contradicts the fact that $J_0(26)$ has a finite quotient over $\mathbb{Q}(\sqrt{-1})$ (see [1] for a proof of this fact).

As a second example, consider the (Thue) Diophantine equation

$$x^n - 3y^n = 2. \tag{8}$$

An obvious solution (for odd n) is with $(x, y) = (-1, -1)$. Using the techniques outlined here, we can show that, for odd $n \geq 3$, there are, in fact, no other integral solutions. For $n = 3$ or 5, this is a consequence of standard computational methods for solving Thue equations. We thus suppose that $n \geq 7$ is prime. We may also assume that a putative solution $(x, y) \neq (-1, -1)$ has both x and y odd. Writing $2 = 2 \cdot 1^m$, we have three options available. If we suppose $m = n$, then $N = 96$. There are two isogeny classes of elliptic curves over $\mathbb{Q}$ at this level, both with full 2-torsion. We are thus unable to use our techniques to derive an immediate contradiction. If we take $m = 2$, we find ourselves at level $N = 768$, where we are again thwarted, this time by the eight isogeny classes of elliptic curves over $\mathbb{Q}$ with conductor 768 and rational 2-torsion. If, however, we let $m = 3$, we find ourselves at level $N \in \{4, 12, 36, 108\}$. By Proposition 4.1, we necessarily have $N = 36$ or $N = 108$. In each case, there is precisely one Galois conjugacy class of cupidal newform at level N, corresponding to elliptic curves with CM by $\mathbb{Q}(\sqrt{-3})$. Applying Proposition 4.2, since $xy \neq \pm 2^r 3^s$ and both $J_0(21)$ and $J_0(39)$ have finite quotients over $\mathbb{Q}(\sqrt{-3})$, we obtain the desired contradiction.

References

[1] M.A. Bennett and C. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.*, to appear.

[2] M.A. Bennett, V. Vatsal and S. Yazdani, Ternary Diophantine equations of signature $(p, p, 3)$, submitted for publication.

[3] C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves over **Q**: wild 3-adic exercises, *J. Amer. Math. Soc.* 14 (2001), 843–939.

[4] J. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.

[5] H. Darmon, On the equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$, *Duke I.M.R.N.* 72 (1993), 263–274.

[6] H. Darmon, The equation $x^4 - y^4 = z^p$, *C.R. Math. Rep. Acad. Sci. Canada* XV (1993), 286–290.

[7] H. Darmon and A. Granville, On the equations $x^p + y^q = z^r$ and $z^m = f(x, y)$, *Bull. London Math. Soc.* 27 (1995), 513–544.

[8] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's Last Theorem, *J. Reine Angew. Math.* 490 (1997), 81–100.

[9] J. Ellenberg, Modular Q-curves and a generalized Fermat equation, in preparation.

[10] W. Ivorra, Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$, preprint.

[11] A. Kraus, Sur les équations $a^p + b^p + 15c^p = 0$ et $a^p + 3b^p + 5c^p = 0$, *C. R. Acad. Sci. Paris Sér. I Math.* 322 (1996), no. 9, 809–812.

[12] A. Kraus, Sur l'équation $a^3 + b^3 = c^p$, *Experiment. Math.* 7 (1998), no. 1, 1–13.

[13] A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, *Canad. J. Math.* 49 (1997), no. 6, 1139–1161.

[14] A. Kraus, On the equation $x^p + y^q = z^r$: a survey, *Ramanujan J.* 3 (1999), no. 3, 315–333.

[15] L. Merel, Arithmetic of elliptic curves and Diophantine equations, *J. Théor. Nombres Bordeaux* 11 (1999), 173–200.

[16] B. Poonen, Some Diophantine equations of the form $x^n + y^n = z^m$, *Acta Arith.* 86 (1998), 193–205.

[17] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J.* 54 (1987), 179–230.

[18] W. Stein, Modular forms database, http://modular.fas.harvard.edu/Tables/

[19] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* (2) 141 (1995), no. 3, 443–551.

Department of Mathematics, University of British Columbia, Vancouver, B.C., V6T 1Z2 Canada

E-mail address: bennett@math.ubc.ca